CLAIMS

We claim:

1. A method for detection and correction of security vulnerabilities in a computing environment, comprising:

analyzing a software solution to identify legal and illegal external interfaces thereto;

attempting to access said software solution using the identified illegal external interfaces; and

storing a record of any illegal external interfaces that allow access to said software solution.

2. The method of claim 1, wherein said software solution comprises at least two independent software programs interacting to form the software solution.

3. The method of claim 1, further comprising:

automatically deploying a corrective measure to said software solution based upon said identified illegal external interface.

4. The method of claim 3, further comprising:

storing each of said corrective measures in a memory.

5. The method of claim 4, further comprising:

making said stored record of illegal external interfaces that allow access, and said stored record of corrective measures available to all users of said detection and correction method, on a global basis.

6. The method of claim 5, wherein said stored record of illegal external interfaces that allow access, and said stored record of corrective measures is made available on a global basis via a network connection.

7. The method of claim 1, wherein said analyzing step includes:

analyzing an XML description of each legal and illegal external interface; and

mapping each legal and illegal external interface into a machine-readable format.

8. A system for detection and correction of security vulnerabilities in a computing environment, comprising:

means for analyzing a software solution to identify legal and illegal external interfaces thereto;

means for attempting to access said software solution using the identified illegal external interfaces; and

means for storing a record of any illegal external interfaces that allow access to said software solution.

9. The system of claim 8, wherein said software solution comprises at least two independent software programs interacting to form the software solution.

10. The system of claim 8, further comprising:

means for automatically deploying a corrective measure to said software solution based upon said identified illegal external interface.

11. The system of claim 10, further comprising:

means for storing each of said corrective measures in a memory.

12. The system of claim 11, further comprising:

means for making said stored record of illegal external interfaces that allow access, and said stored record of corrective measures available to all users of said detection and correction method, on a global basis.

13. The system of claim 12, wherein said stored record of illegal external interfaces that allow access, and said stored record of corrective measures is made available on a global basis via a network connection.

14. The system of claim 8, wherein said analyzing means includes:

means for analyzing an XML description of each legal and illegal external interface; and

means for mapping each legal and illegal external interface into a machine-readable format.

15. A computer program product for detection and correction of security vulnerabilities in a computing environment, the computer program product comprising a

computer-readable storage medium having computer-readable program code embodied in the medium, the computer-readable program code comprising:

computer-readable program code that analyzes a software solution to identify legal and illegal external interfaces thereto;

computer-readable program code that attempts to access said software solution using the identified illegal external interfaces; and

computer-readable program code that stores a record of any illegal external interfaces that allow access to said software solution.

16. The computer program product of claim 15, wherein said software solution comprises at least two independent software programs interacting to form the software solution.

17. The computer program product of claim 15, further comprising:

computer-readable program code that automatically deploys a corrective measure to said software solution based upon said identified illegal external interface.

18. The computer program product of claim 17, further comprising:

computer-readable program code that stores each of said corrective measures in a memory.

19. The computer program product of claim 18, further comprising:

computer-readable program code that makes said stored record of illegal external interfaces that allow access, and said stored record of corrective measures available to all users of said detection and correction method, on a global basis.

20. The computer program product of claim 19, wherein said stored record of illegal external interfaces that allow access, and said stored record of corrective measures is made available on a global basis via a network connection.

21. The computer program product of claim 15, wherein said computer-readable program code for analyzing the software solution includes:

computer-readable program code that analyzes an XML description of each legal and illegal external interface; and

computer-readable program code that maps each legal and illegal external interface into a machine-readable format.